

Are You Ready for an SIS?

**What to do before starting on
your SIS...and after it's installed**

March 24, 2009



BLUEFIELD
PROCESS SAFETY

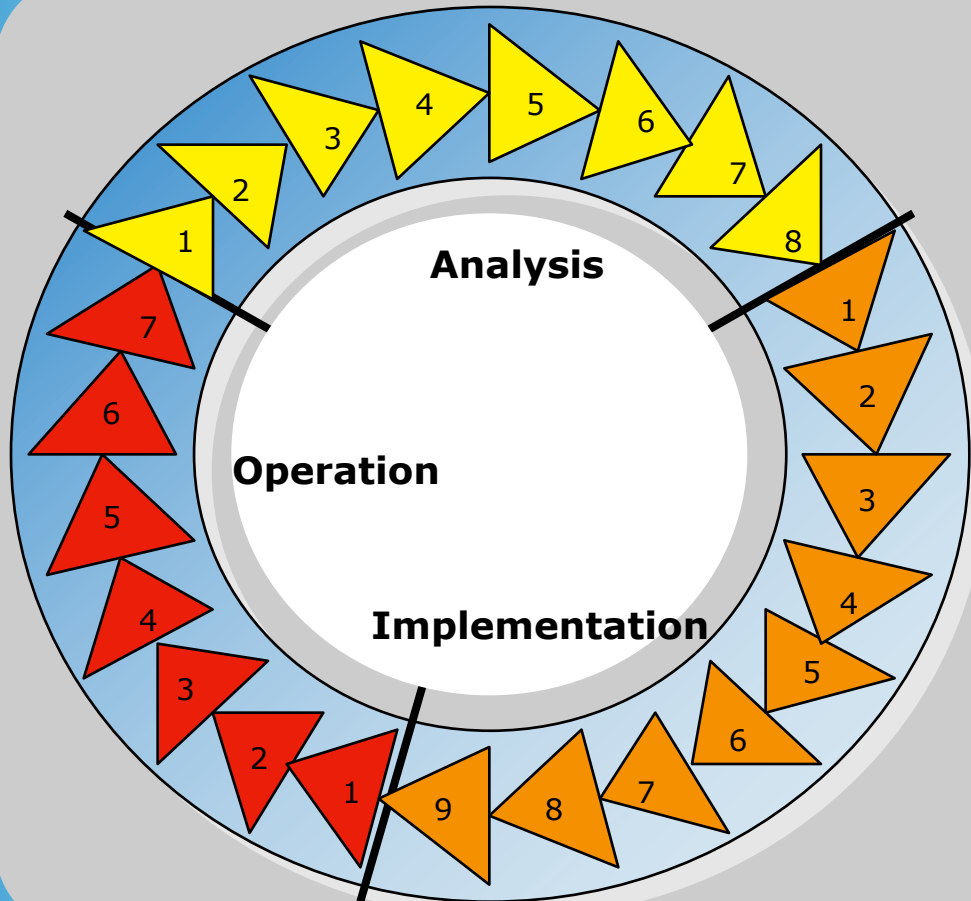
Presenter: Mike Schmidt, P.E.

- ❖ Principal
Bluefield Process Safety
- ❖ Principal Safety Consultant
Emerson Process Management

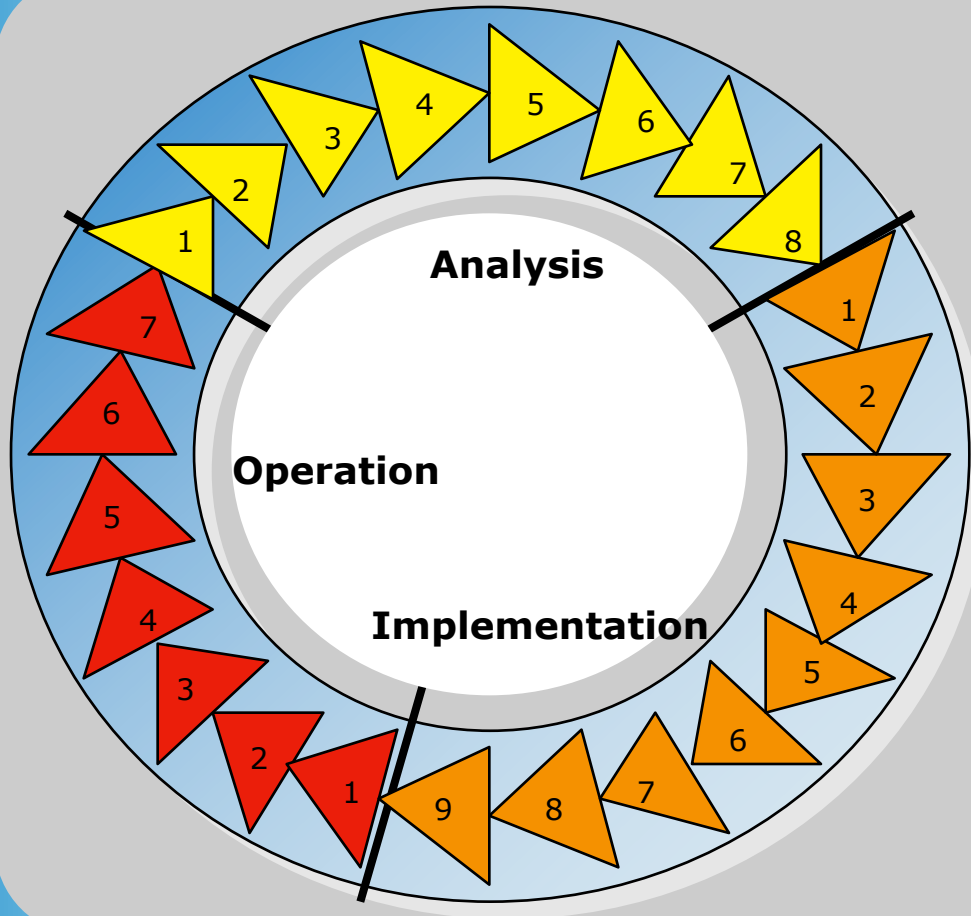
Before starting on an SIS

- ❖ Steps of the Safety Life Cycle and Why They Matter
- ❖ SIFs and SIL Assignment
- ❖ The SRS
- ❖ After the SIS is installed
 - a conversation

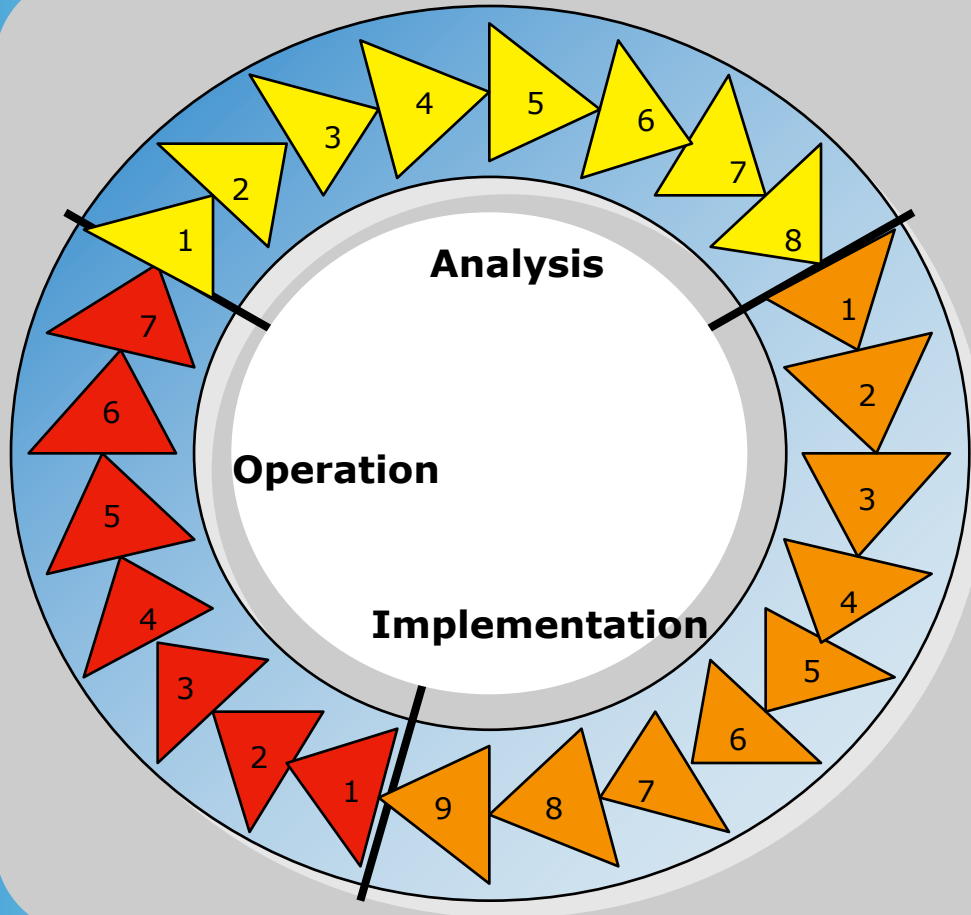
The Safety Life Cycle



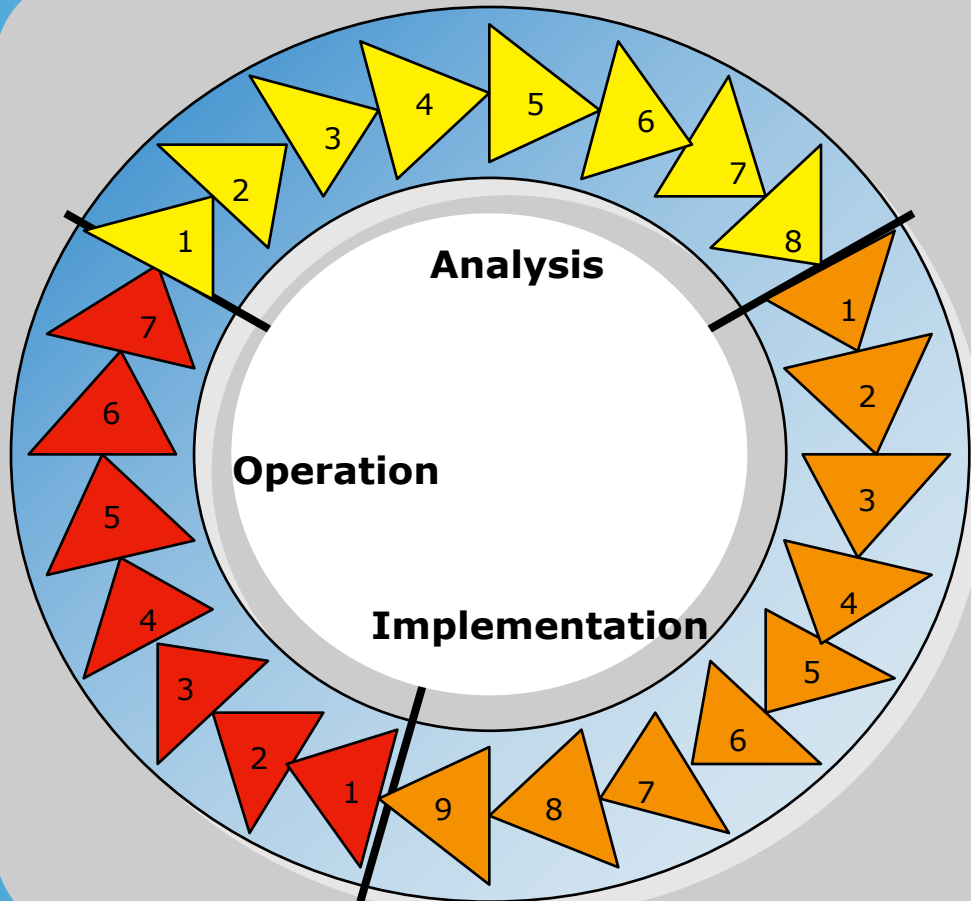
The Safety Life Cycle



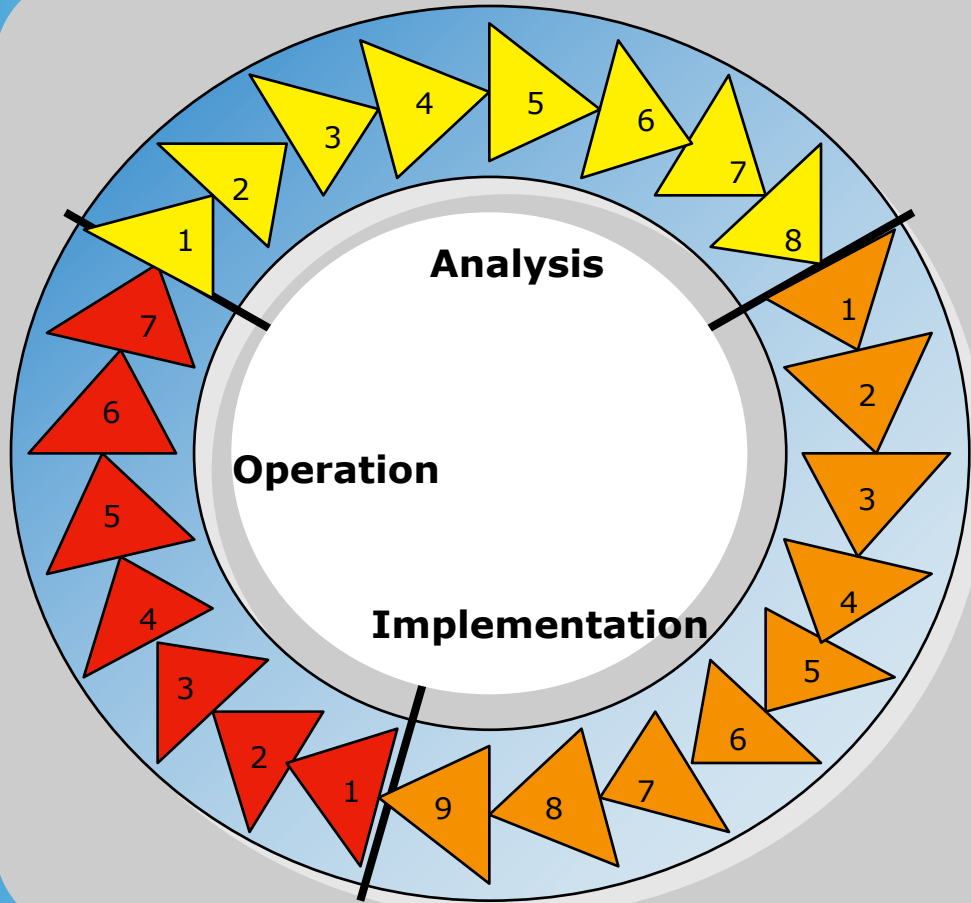
The Safety Life Cycle



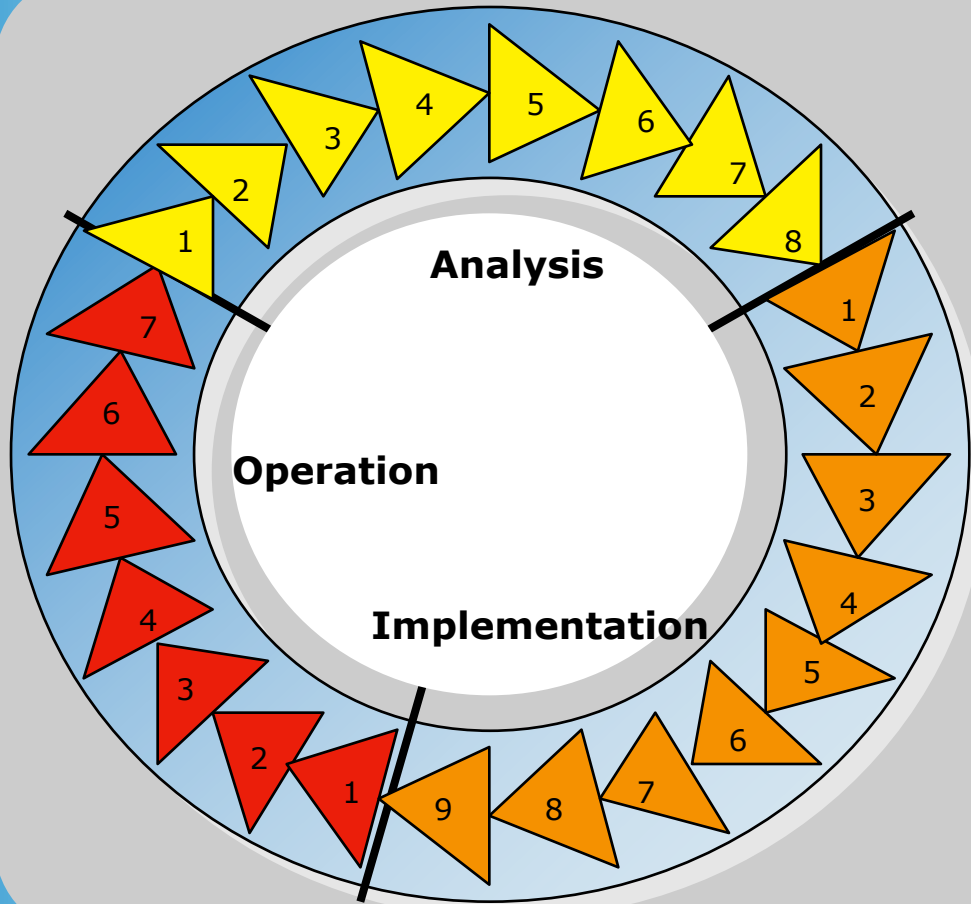
The Safety Life Cycle



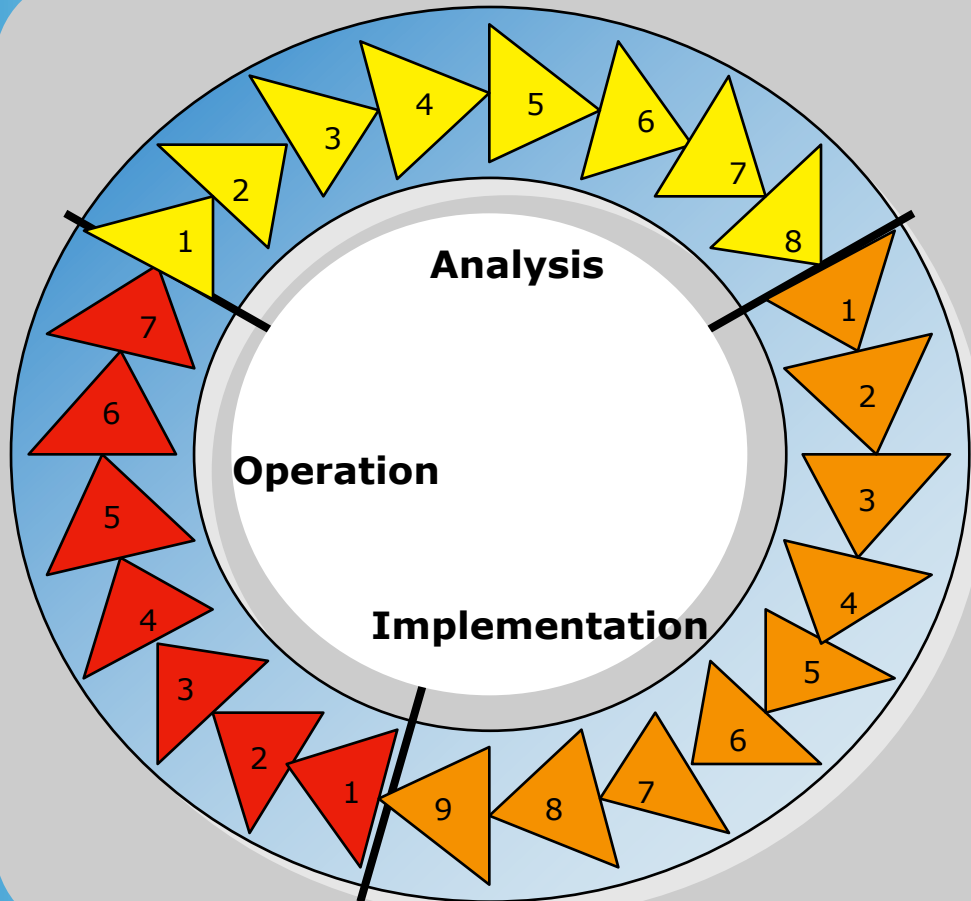
The Safety Life Cycle



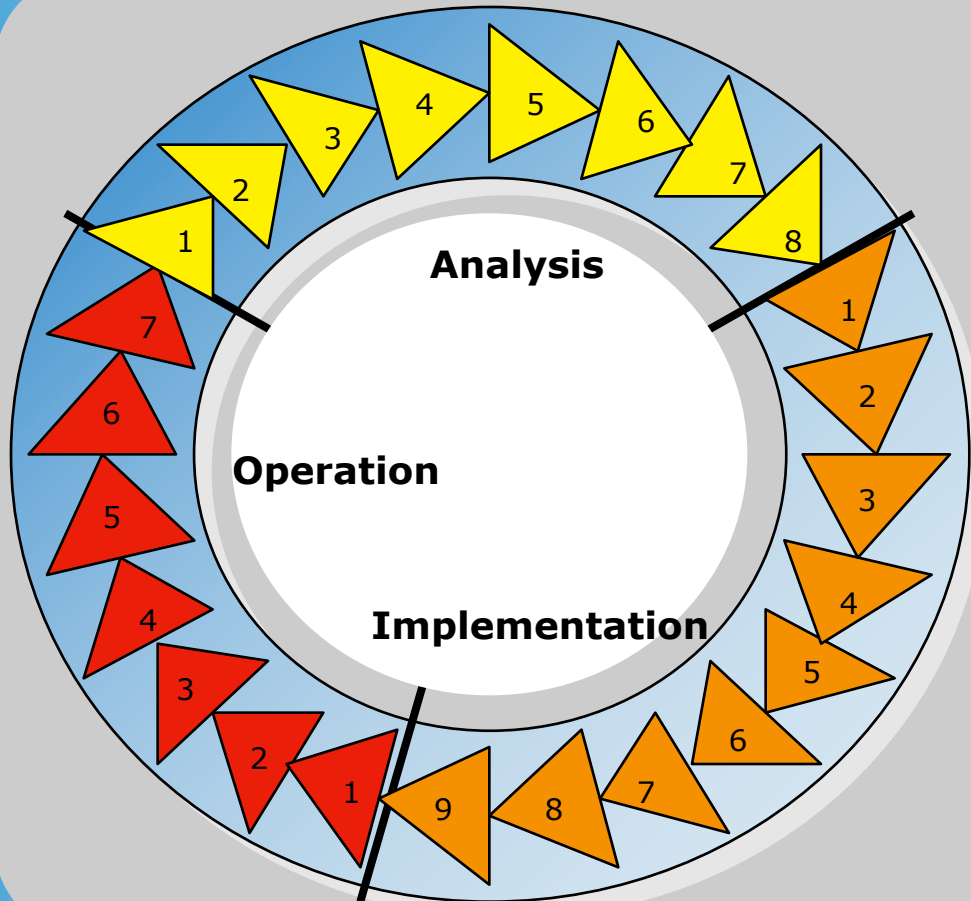
The Safety Life Cycle



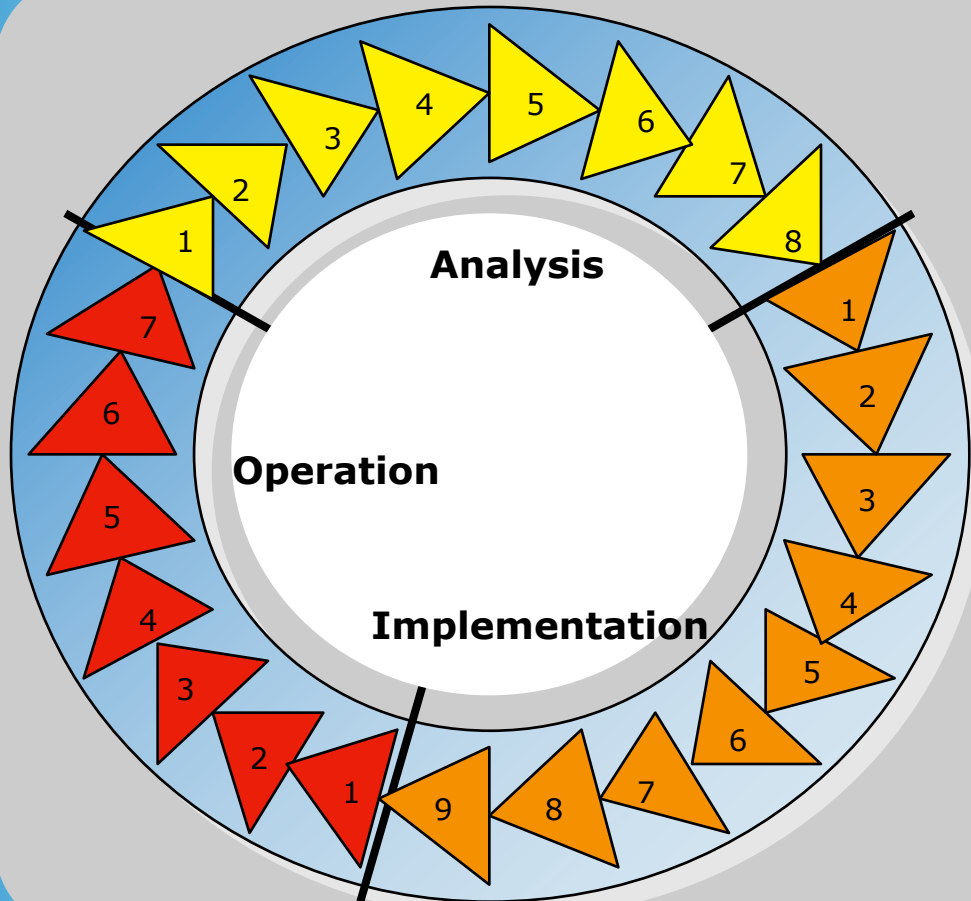
The Safety Life Cycle



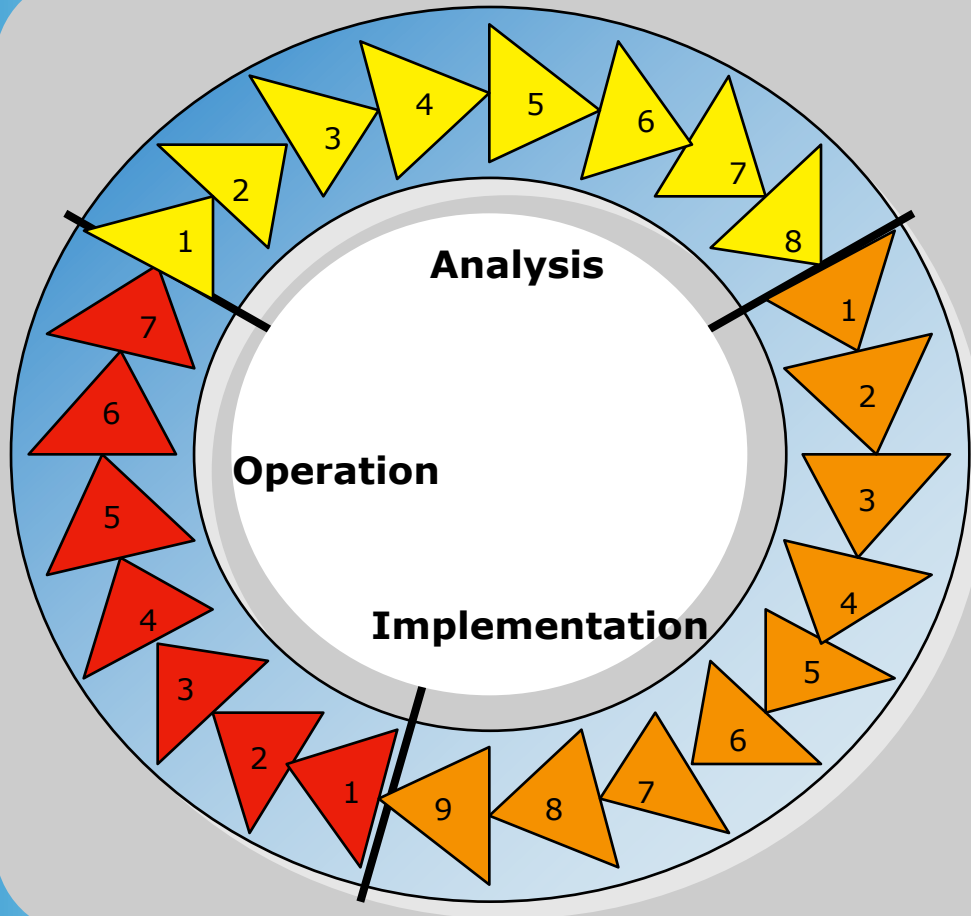
The Safety Life Cycle



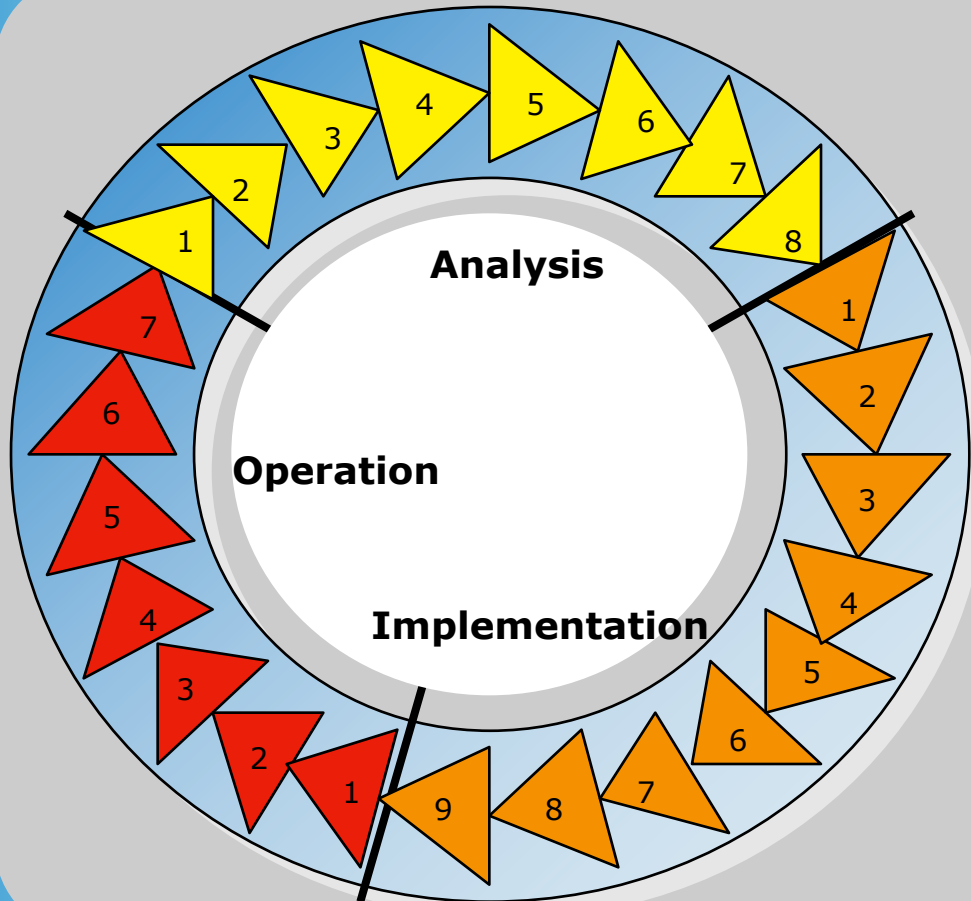
The Safety Life Cycle



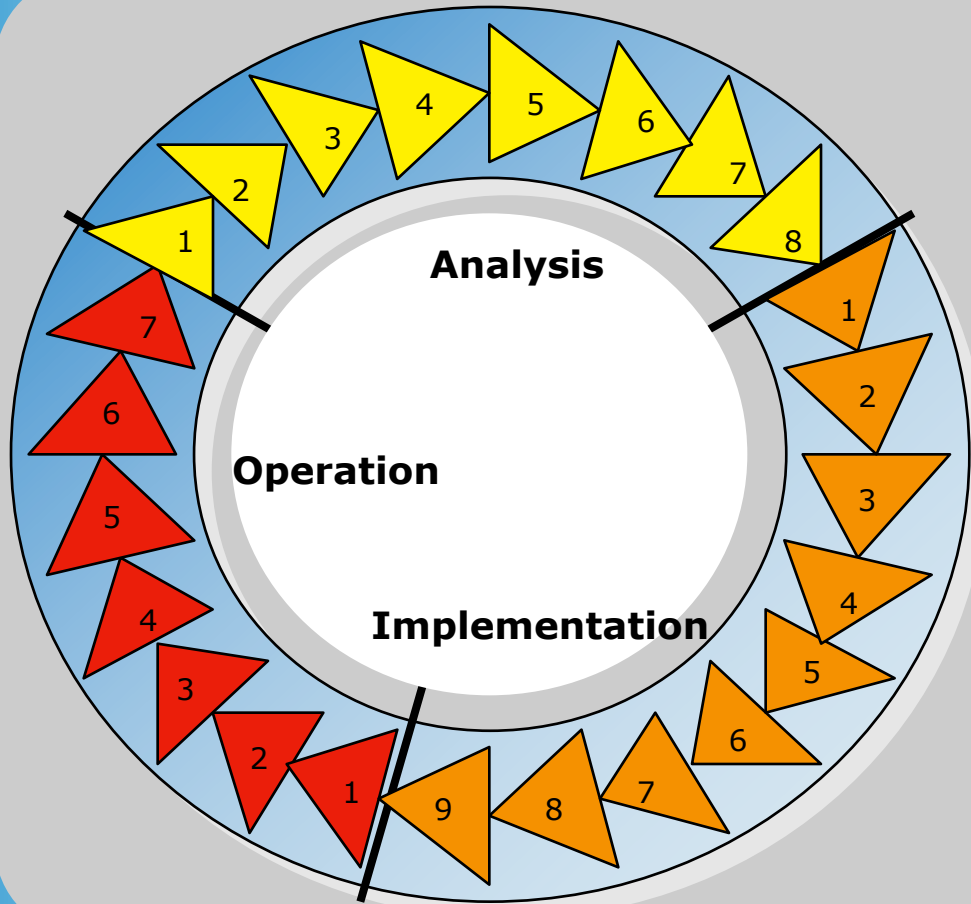
The Safety Life Cycle



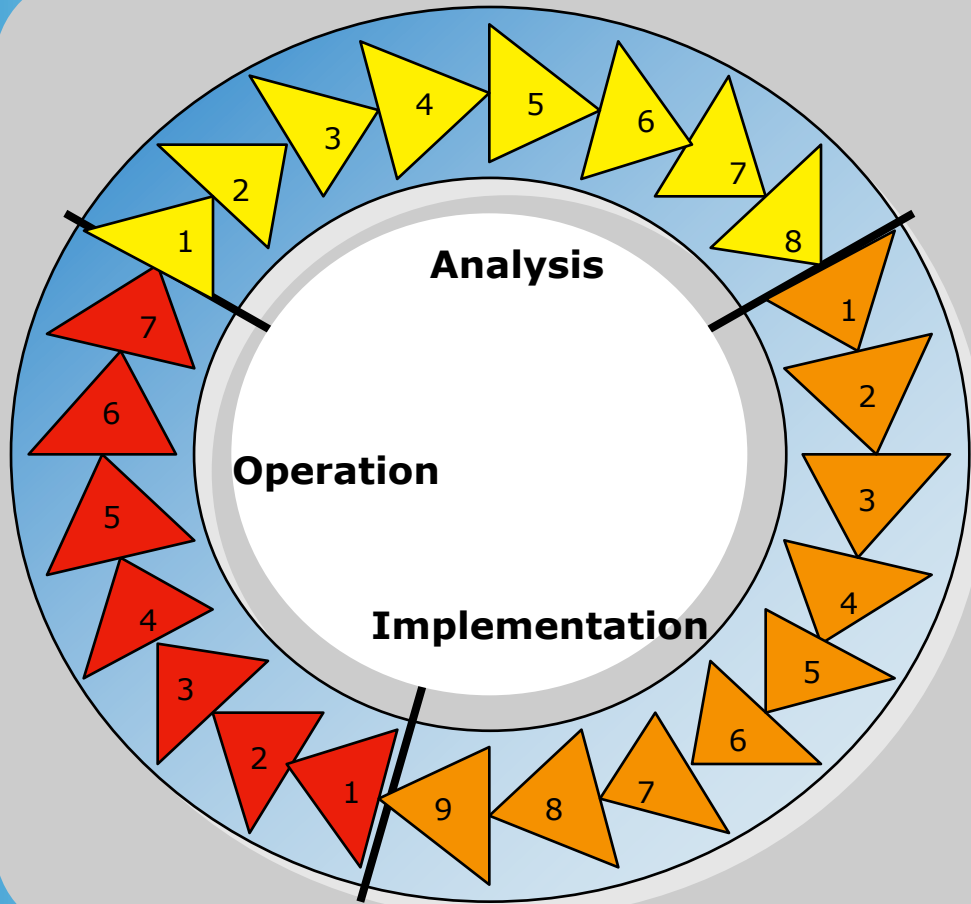
The Safety Life Cycle



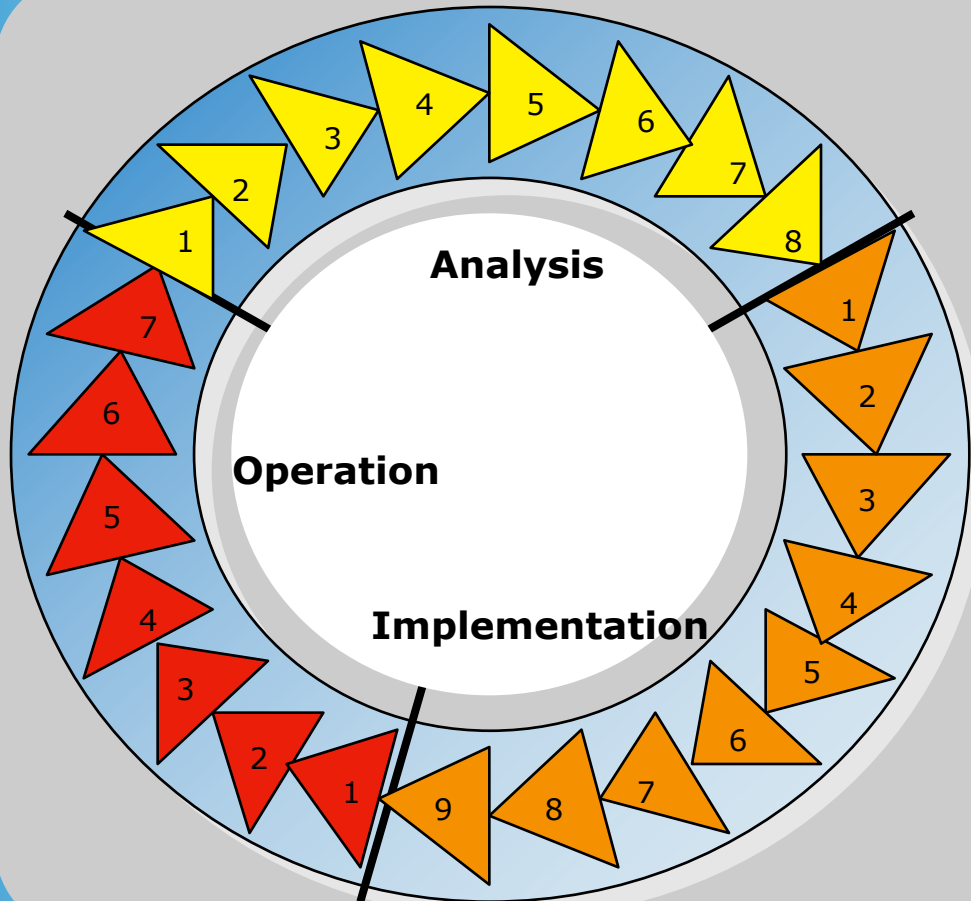
The Safety Life Cycle



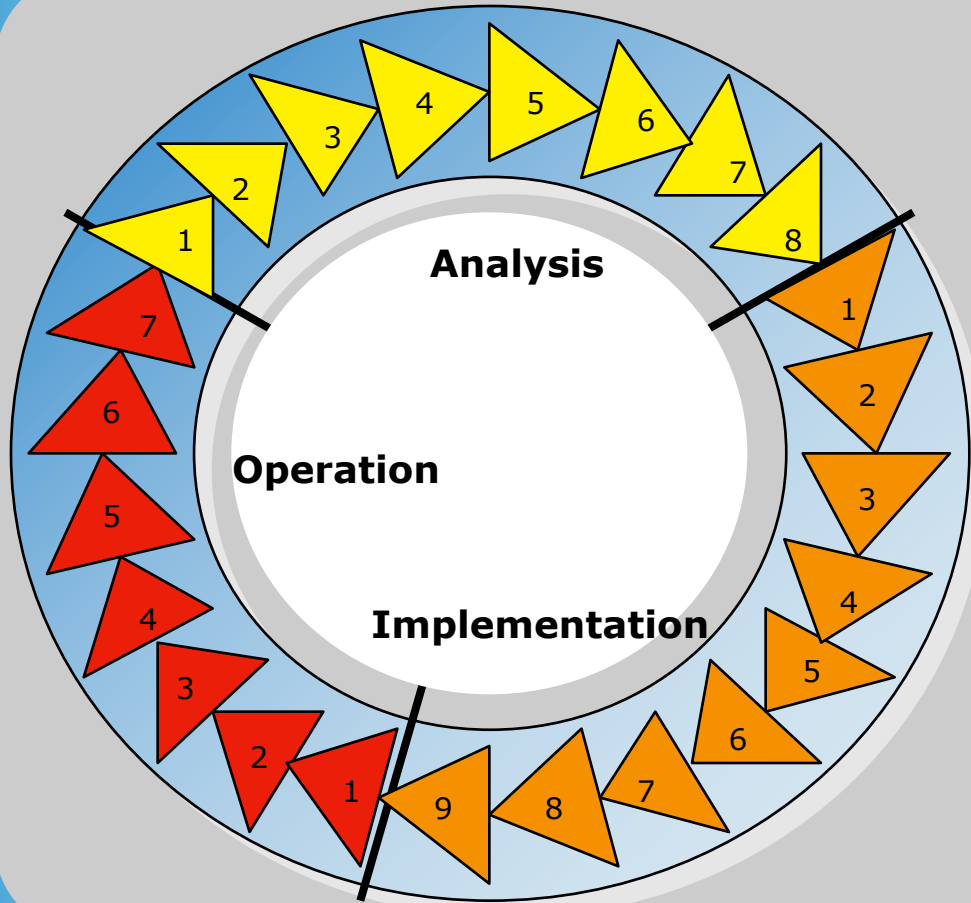
The Safety Life Cycle



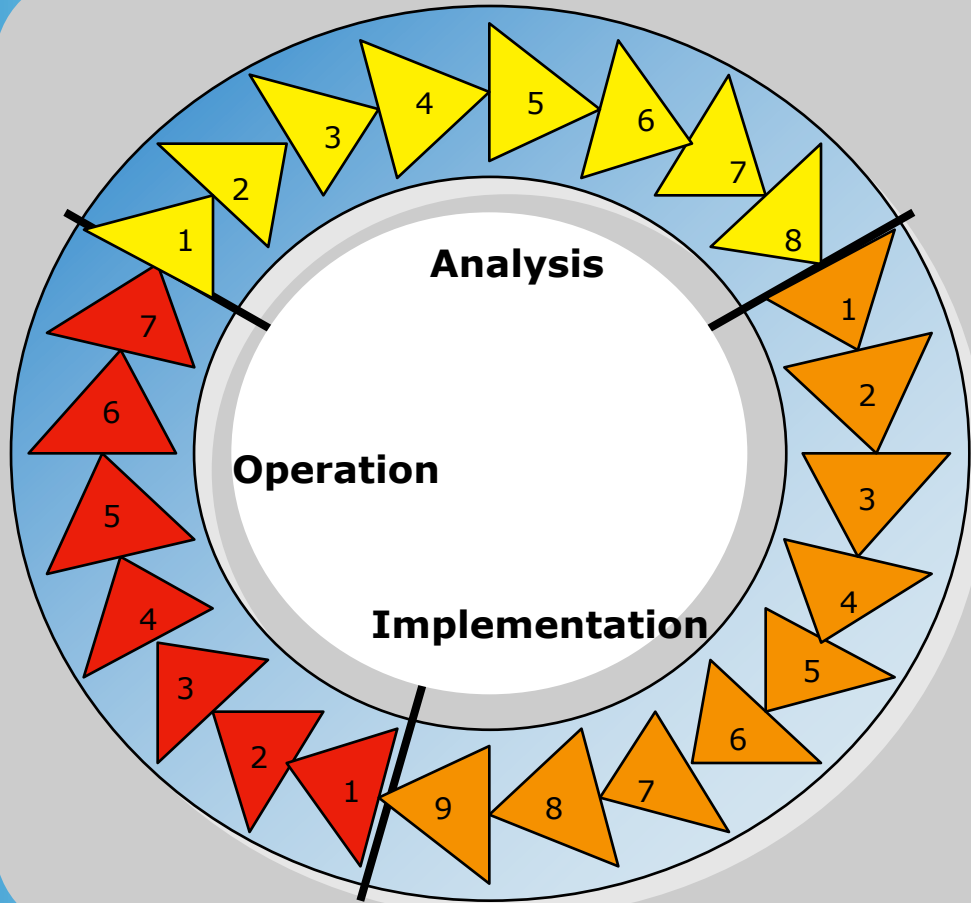
The Safety Life Cycle



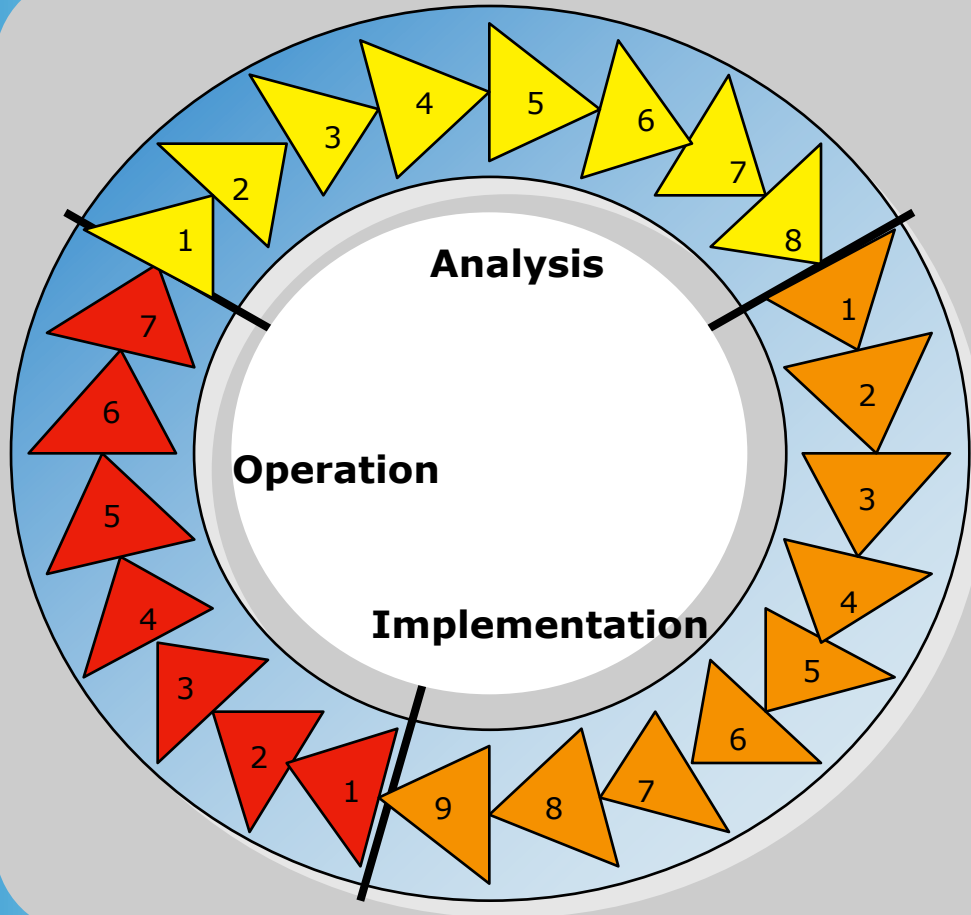
The Safety Life Cycle



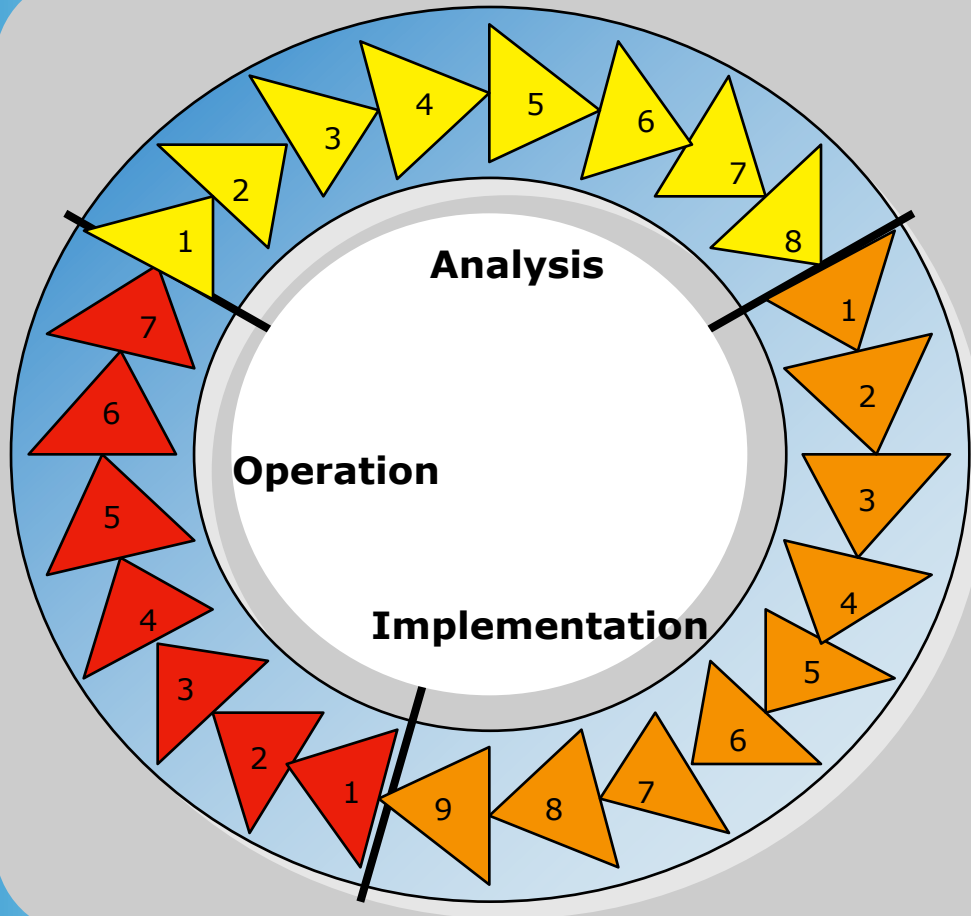
The Safety Life Cycle



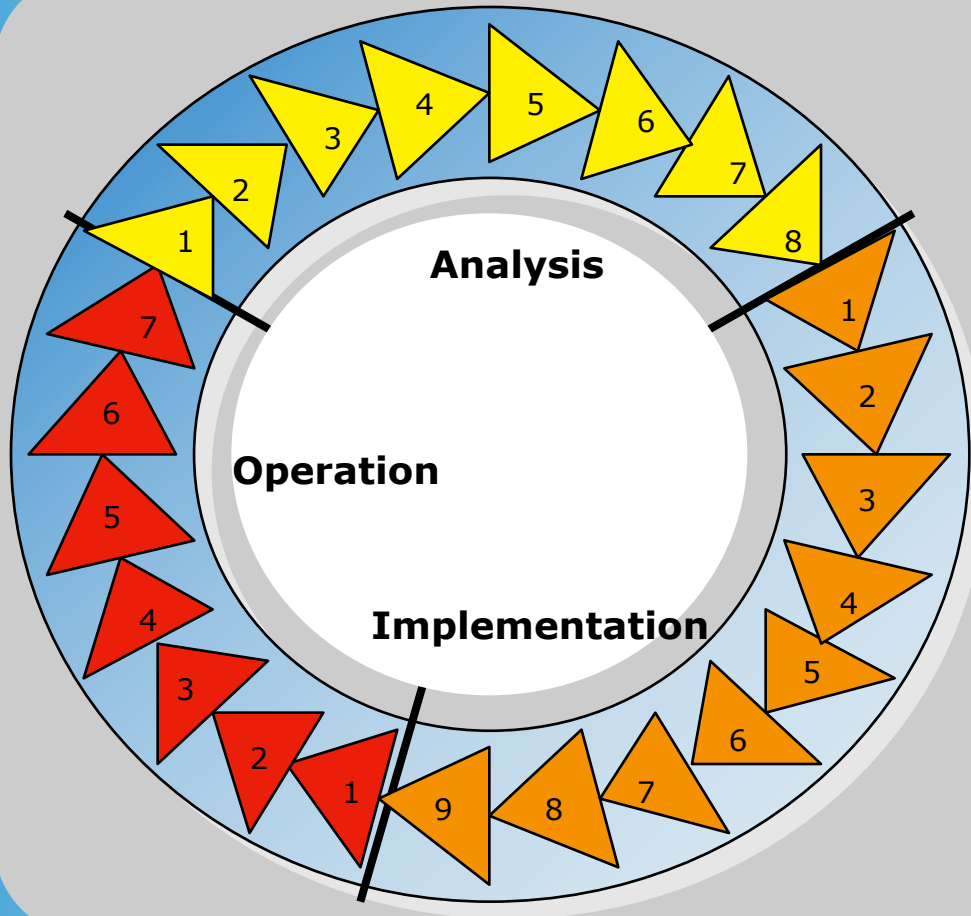
The Safety Life Cycle



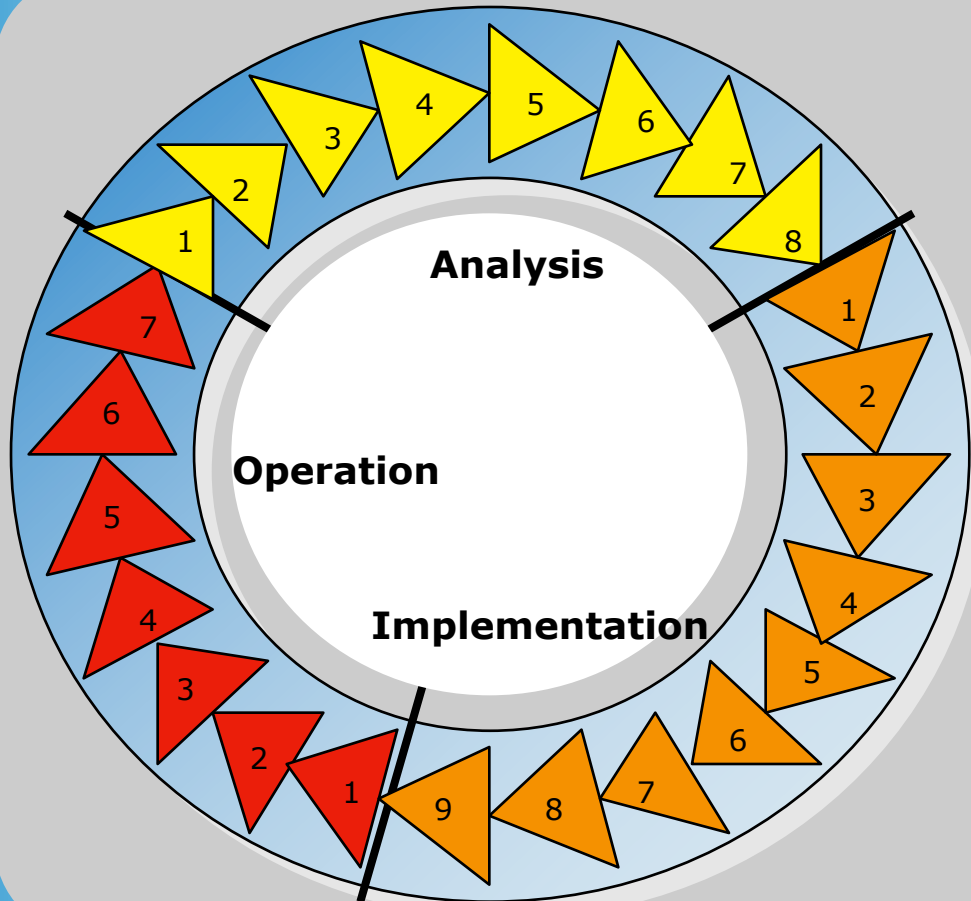
The Safety Life Cycle



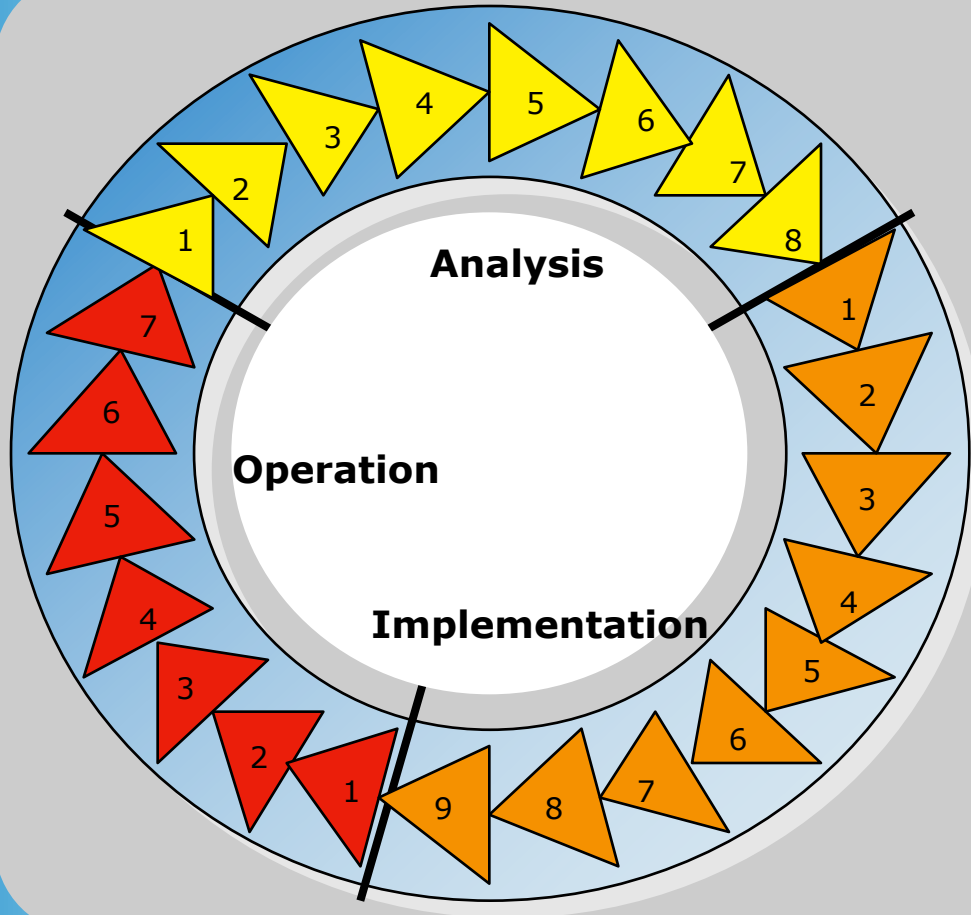
The Safety Life Cycle



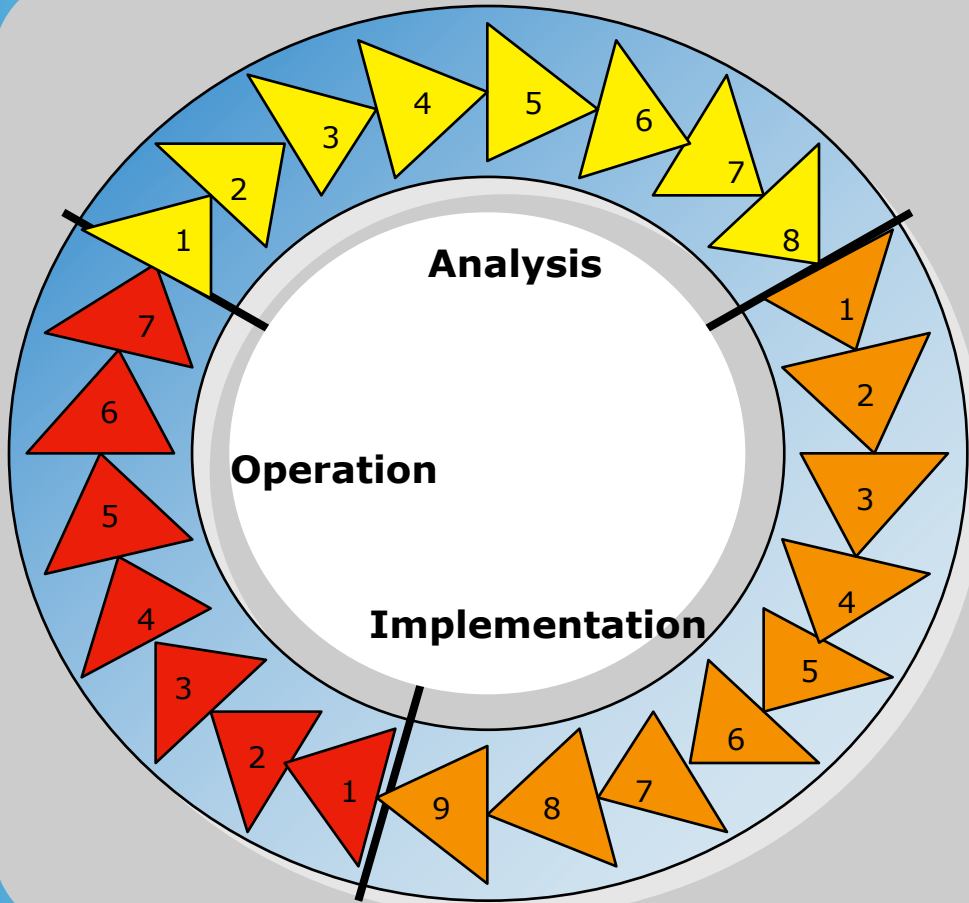
The Safety Life Cycle



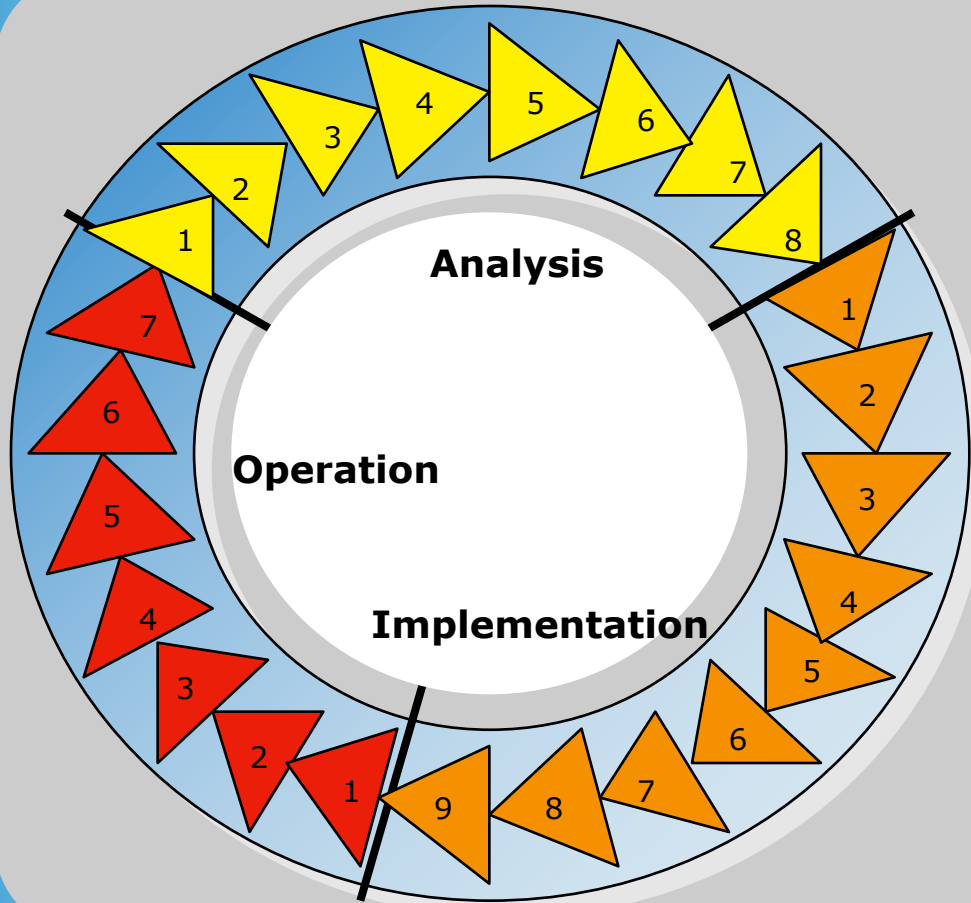
The Safety Life Cycle



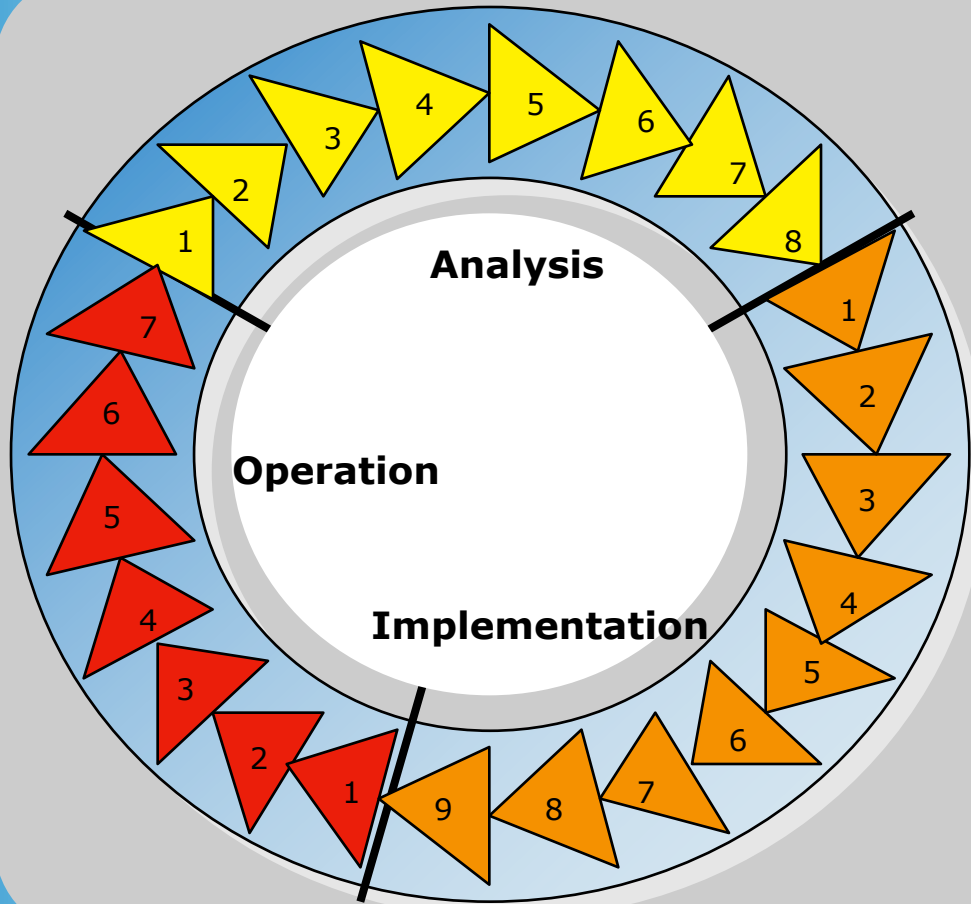
The Safety Life Cycle



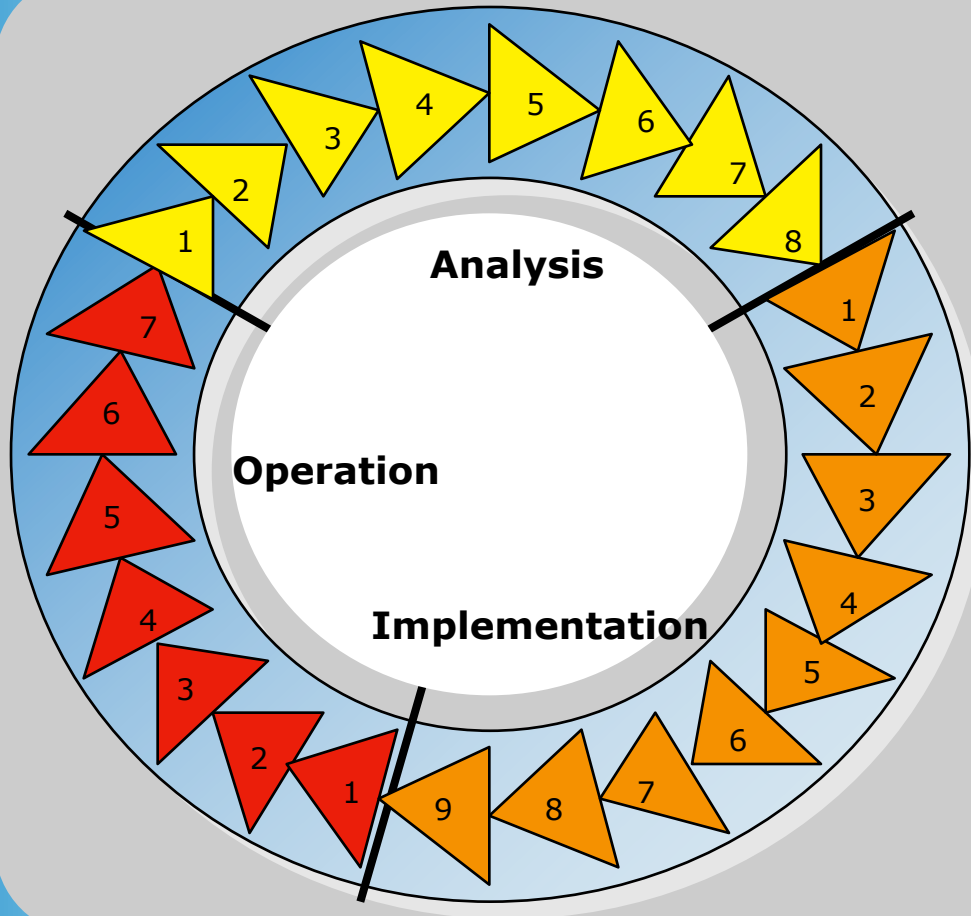
The Safety Life Cycle



The Safety Life Cycle



The Analysis Phase



Process Design

- ❖ Process Design has the greatest influence on the need for an SIS
- ❖ This includes all of the main Process Design Documents
 - ◆ *Conceptual Design*
 - ◆ *PFDs and Heat/Material Balances*
 - ◆ *P&IDs*

Hazard Identification

- ❖ Hazards are identified during the Process Hazard Analysis (PHA)
- ❖ Preliminary PHAs
 - ◆ *"What If?"*
 - ◆ *Checklist*
- ❖ Detailed PHA
 - ◆ *HazOp (Hazard Operability Review)*

HazOps: Some tips

HazOp: Worksheets


Bluefield Process Safety Corp. No. 00000
 ABC Chemical Co. - Pulp Plant
 Unit: Process Reactor

Doc. No.: 00000
 Rev. No.: 0
 Date: 00/00/0000

Node: (00000-1) Process Reactor & 100-1000

Deviation	Cause	Consequences	Safeguards/Recommendations	By
Pressure - high				
Pressure - low				
Pressure - surging				
Temp - high				
Temp - low				
Flow - high				
Flow - low				
Flow - reverse				
Flow - surging				
Flow - other than (loss of containment)				
Level - high				
Level - low				
Level - other than (loss of containment)				
Comp - high				
Comp - low				
Comp - other than (containment)				

Page 1 of 1

 BLUEFIELD
PROCESS SAFETY

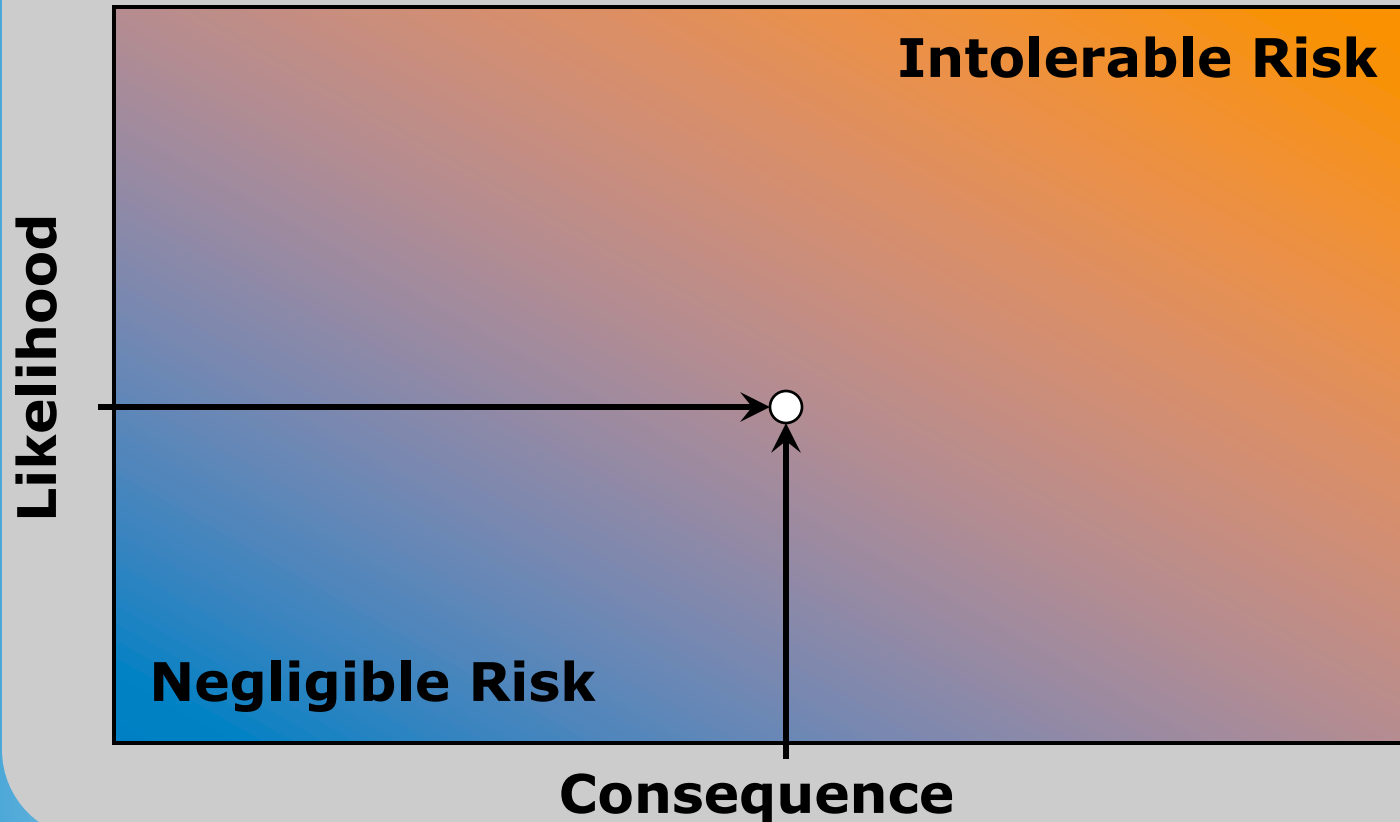
Tip 1. Take care in identifying the cause. If it's a deviation, that normally means a failure.

Tip 2. Some HazOp methods prompt an identification of frequency. If this is done, do it consistently...with or without safeguards, with or without recommendations, with or without SIFs



Risk Assessment

$$\text{Risk} = \text{Consequence} \times \text{Likelihood}$$



Risk Assessment

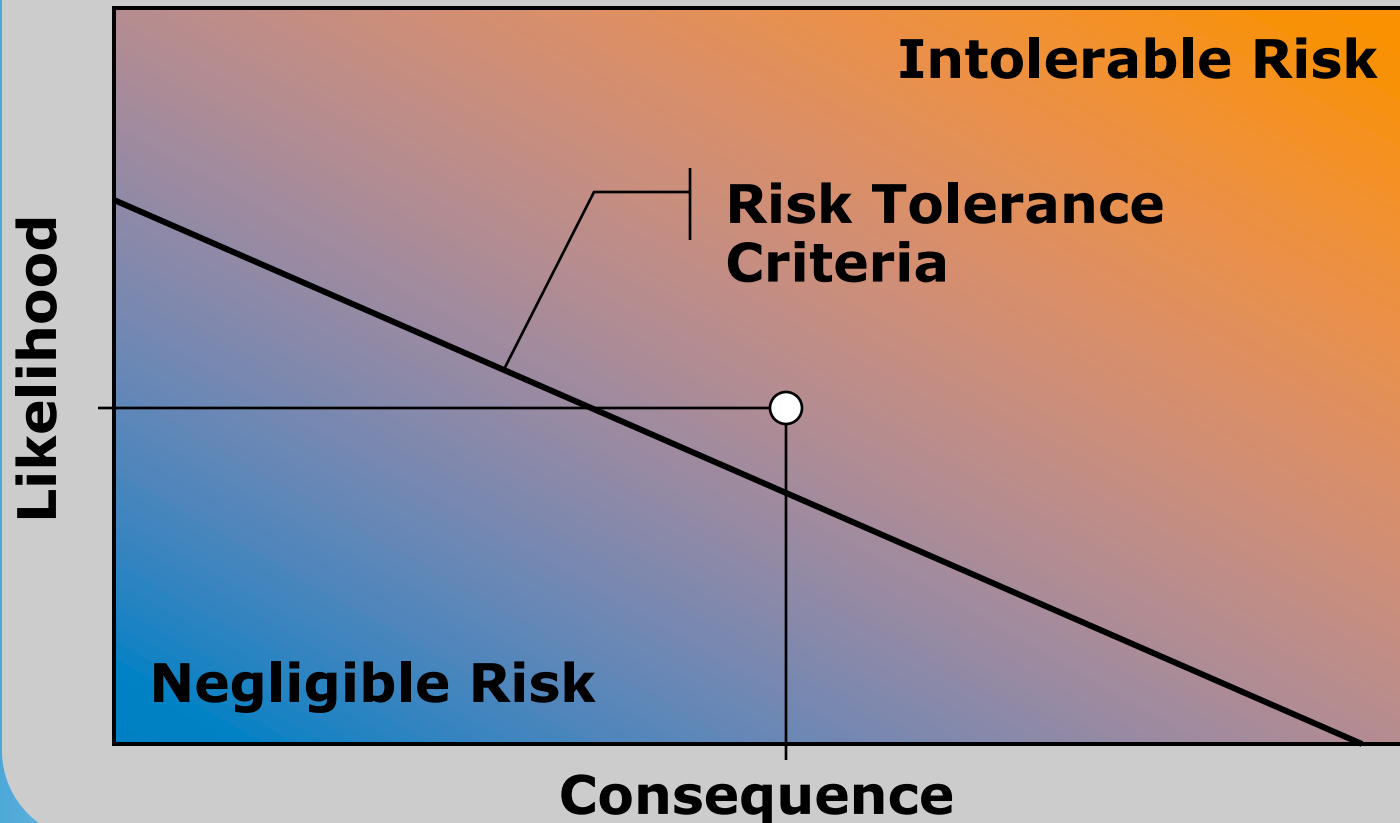
- ❖ Consequence Analysis
 - ◆ *Offsite Consequence Analysis (OCA)*
 - ◆ *Quantitative Risk Analysis (QRA)*

- ❖ Likelihood Analysis
 - ◆ *Layers of Protection Analysis (LOPA)*



How much risk is too much?

Compare: **Risk against Risk Tolerance Criteria**



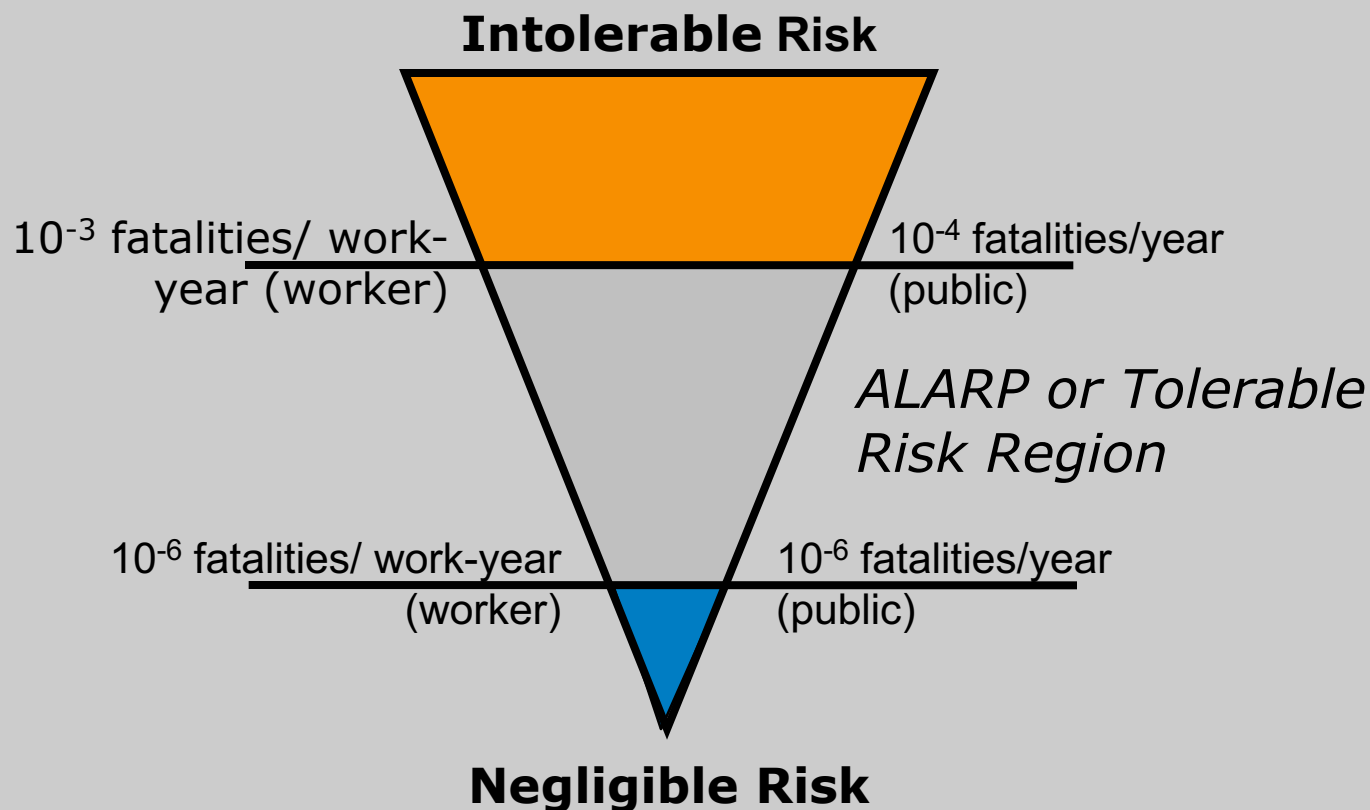
Risk Tolerance Criteria

- ❖ May come from any of several sources
 - ◆ *Plant policy*
 - ◆ *Corporate policy*
 - ◆ *Industry benchmarks and guidelines*
 - ◆ *Government mandates*

- ❖ The United States does not set tolerable risk levels or offer guidelines.

- ❖ Outside consultants should not decide for you what is tolerable

ALARP: Levels in the UK



Factors to Consider

- ❖ Number of facilities
- ❖ Multi-national or not
- ❖ Societal expectations

Large, multinational companies tend to set levels consistent with international mandates, while smaller companies tend to operate in wider ranges and implicitly, at higher levels of risk

Risk Reduction Allocation

When additional risk reduction is required

- ❖ Non-instrumented IPLs

- ◆ *Passive components:*

- Dikes
 - Blast walls
 - Secondary containment

- ◆ *Active components:*

- Relief devices
 - Redundant equipment or installed spares

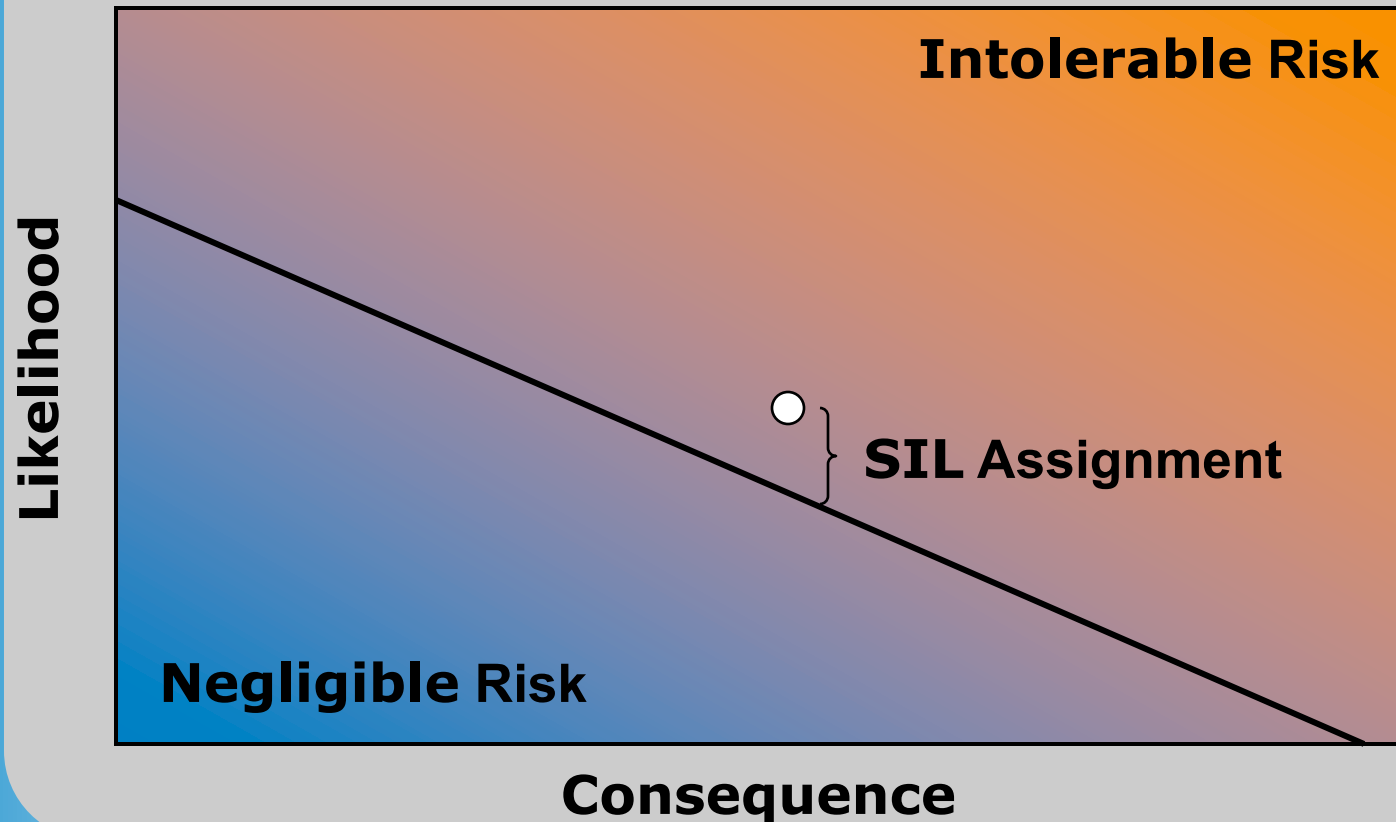
- ❖ Instrumented IPLs

- ◆ *Control loops within the BPCS*

- ◆ *Safety Instrumented Functions*

How much risk reduction?

SIL: Difference Between Risk and Risk Tolerance Criteria



Safety Function Definition

- ❖ Non-SIS Safety Functions (IPLs):
 - ◆ *Scope definition*
 - ◆ *Project specification*(This follows the normal project cycle)

- ❖ SIS:
 - ◆ *SIF List*
 - ◆ *SIL assignment*

Note: SILs are assigned to functions, not to systems

SIF List

Typically includes

- ❖ SIF Tag
- ❖ Hazard Description
- ❖ SIL Assignment/Required PFDavg
- ❖ Trip conditions
 - ◆ *Instrument tags*
 - ◆ *Set point and direction*
 - ◆ *Voting*
- ❖ Trip actions
 - ◆ *Instrument tags*
 - ◆ *Trip state*



Safety Function Specification

- ❖ For an SIS, this is the Safety Requirements Specification – the SRS
 - ◆ *Used to develop system quotes*
 - ◆ *Basis of detailed design*
 - ◆ *Basis of configuration*
- ❖ More extensive than a SIF List



The SRS – §10.3.1

“These requirements shall be sufficient to design the SIS and shall include the following:”

- ❖ A list of 27 bullet items follow
- ❖ The SIF List addresses five of them



The SRS – §10.3.1

Other items include

- ❖ Source of demand and demand rate
- ❖ Proof test intervals
- ❖ Response time intervals
- ❖ Energize-to-trip or de-energize-to-trip
- ❖ Maximum allowable spurious trip rate
- ❖ Overrides/inhibits/bypasses
- ❖ Resets
- ❖ Dangerous combinations



Organizing an SRS

Suggested approach

- ❖ General SIS Requirements
- ❖ Specific SIF Requirements
- ❖ Basis of Design
 - ◆ *Policies*
 - ◆ *Procedures*
 - ◆ *Documents*
 - ◆ *Reports*



General SIS Requirements

SRS: General SIS Requirements

CONTENTS

- 1. PROJECT OVERVIEW
- 1.1. PROJECT INTRODUCTION
- 1.1.1. Project Purpose
- 1.1.2. Safety Logic Solver
- 1.1.3. Regulations and Requirements
- 1.2. Project Description
- 1.2.1. Project Approach
- 1.2.2. Project Personnel and Organization
- 1.2.3. Project Description - Operations and Maintenance
- 1.2.4. Environmental Considerations
- 2. GENERAL TERMINOLOGY
- 2.1. Acronyms
- 2.2. Terms and Definitions
- 3. GENERAL FUNCTION
- 3.1. Risk Reduction
- 3.1.1. Risk Reduction Table
- 3.1.2. Architecture and Functional Requirements
- 3.2. Separate Hazards
- 3.3. Common Cause Failure
- 3.4. General Functional Requirements
- 3.4.1. Demand Rate
- 3.4.2. Modes of Operation
- 3.4.3. Response Time
- 3.4.4. Maximum Allowable Protection Principle
- 3.4.5. Fault Detection
- 3.4.6. Human Factors
- 3.4.7. Hazards
- 3.4.8. Proof Test Intervals
- 3.4.9. Redundancy
- 3.4.10. Special Circumstances
- 3.4.11. Manual Shutdown
- 3.5. Special Circumstances
- 3.5.1. For Successful Operation
- 3.5.2. To Address Escalation
- 3.5.3. To Survive a Major Accident
- 3.6. Field Devices
- 3.6.1. Third-Party Certified Smart Sensors
- 3.6.2. Smart Sensors
- 4. SYSTEM REQUIREMENTS
- 4.1. Integration to Other Systems
- 4.1.1. Interfaces
- 4.1.2. Integration
- 4.1.3. Off-site Emergency Response
- 4.1.4. Operator Interface to Process Alarms
- 4.2. Operator Interfaces
- 4.2.1. Operator Display Unit
- 4.2.2. Color Conventions
- 4.2.3. Alarm Color Standards
- 4.3. Data Acquisition and Continuous Data Archiving
- 4.3.1. Data Archiving and Retrieval
- 4.3.2. Data Archiving and Retrieval
- 4.3.3. Physical Security Data
- 5. BASIS OF DESIGN
- 5.1. Process Technology
- 5.1.1. Process Design and Project Drawings
- 5.1.2. Piping and Instrumentation Diagrams
- 5.1.3. Plot Plans and Equipment Electrical Area Classification
- 5.2. Utility Supply Information
- 5.2.1. Power Distribution
- 5.2.2. Instrumented Air
- 5.2.3. Cooling Water
- 5.2.4. Refrigeration
- 5.2.5. Other
- 5.3. Procedures
- 5.3.1. Start-up Procedures
- 5.3.2. Maintenance Procedures
- 5.3.3. Analysis and Allocation of Process Hazard Analysis
- 5.3.4. Process Risk Analysis
- 5.3.5. HOP List
- 5.3.6. SIL Classification Report
- 5.4. Control System Design
- 5.4.1. SIS Specification
- 5.4.2. System Architecture
- 5.4.3. Logic Solver Specification
- 5.4.4. Application Software Specification
- 6. SRS DATABASE
- 7. DOCUMENT CONTROL
- 7.1. Approvals
- 7.2. Revision History

7 DOCUMENT CONTROL

7.1 Approvals

Process Safety _____ Date: _____
Signature by Process Safety representative indicates that the document has been reviewed and approved for use as basis for SIS design and operation.

Facility Representative _____ Date: _____
Signature by facility representative indicates that the document has been reviewed and approved for use as basis for SIS design and operation.

Project Manager _____ Date: _____
Signature by Project Manager indicates that the document has been reviewed and approved for use as basis for SIS design and operation.

7.2 Revision History

Revision	Revision Date	Revised By	Revision Description
A	30-May-2008	Mike Schmidt	Initial issue

***END OF DOCUMENT ***

Rev B, DD-Mon-YYYY Page 22 of 25

BLUEFIELD PROCESS SAFETY



Specific SIF Requirements

Datasheet: SIF

Bluefield Process Safety Proj. No.: **1234567** Rev: **A**
ABC Company Area 1 SIS Rev. Date: **3/9/2006**
 Location: **Anytown, USA** By: **John Doe**

Target: Achieved **SIF # 1** P&ID Dwg. No.: 100
 SIL: 1
 PFD: 0.017 Hazard: **Overflow of Process Tank containing flammable materials resulting in ignition of flammable vapors and flash fire, leading to fatality due to exposure to fire.**
 MTTFs: 0.2 yr

Purpose: Prevent overflow of Process Tank, 101.

Always Enabled

S F

Stage 1 Action: On high level, close all inlet valves from feed sources greater than 10% of Process Tank volume.
 Stage 2 (For SIL verification calculations, only one valve is open at a time, even though the SIF doses all valves.)
 Stage 3
 Stage 4
 Stage 5
 Stage 6
 Stage 7
 Stage 8

Function: 1oo1 voting by high level switch. 5 sec delay. First out stays on graphic. Single block valve on each inlet gives 1oo1 voting on final elements.

On Fault: For sensor, stop batch and notify operator. For final elements, stop batch and notify operator.

Notes:

Reset: Manual

Bypass: Device/Forced

Demand: 0.1 /yr

Trip: De-energize to trip

Bypass Clear: Auto 72hr

Mode: Low demand

Response: 500 ms

Rev No.: A

Causes	Set Point	Units	Proof Test	Effects	Safe Action	Group	Proof Test
LSHH--1	Not equal to On	-	365				
				XV-01 Valve #1	Closed	1	365
				XV-02 Valve #2	Closed	1	365
				XV-03 Valve #3	Closed	5	365
				XV-04 Valve #4	Closed	5	365
				XV-05 Valve #5	Closed	5	365
				XV-06 Valve #6	Closed	5	365

Printed on 3/23/2009
Rev A

Page 1 of 5



Reliability Verification

Two kinds of "SIL Calcs"

- ❖ SIL Assignment Calculations
 - ◆ *Consequence Analysis*
 - ◆ *Likelihood Analysis*
- ❖ SIL Verification Calculations
 - ◆ *Required by standards*
 - ◆ *Use a combination of software tools and custom calculations*
 - exida – SILVER (exSILentia)
 - SIS-Tech – SiLSOLVER

Before starting SIS design

- ❖ Process Design
- ❖ Hazard Identification
- ❖ Risk Assessment
- ❖ Risk Tolerance Criteria Confirmation
- ❖ Risk Reduction Allocation
- ❖ Safety Function Definition
- ❖ Safety Requirements Specification
- ❖ Reliability Verification

After the SIS is installed

Are there questions about:

- ❖ Witnessing
- ❖ Procedures
- ❖ Responsibility (Vendor or customer?)
- ❖ Certificates
- ❖ Frequency
- ❖ Training after installation
(Who needs it? Who can operate?)